WorksPad™

Руководство по установке и конфигурированию

Версия для Linux

Версия 5.2.2 – Сентябрь 2022

Официальный веб-сайт: http://www.workspad.ru.

Содержание

1. Введение

WorksPad представляет собой клиент-серверную систему удалённого доступа с мобильных устройств к ресурсам корпоративной сети организации.

Клиентское приложение WorksPad позволяет получить доступ с мобильных устройств по сети Интернет к почтовым службам, файловым хранилищам, веб-ресурсам, размещенным внутри корпоративной сети, без необходимости публикации таких ресурсов в Интернет.

Серверная часть системы реализована в виде набора компонентов, работающих под управлением операционных систем семейства Linux. В рамках данного руководства в качестве целевой ОС рассматривается Debian.

Пользователями системы WorksPad могут быть только пользователи домена LDAP.

Данный документ описывает требования, настройки и действия, необходимые для развёртывания серверной части системы WorksPad в корпоративной сети организации.

2. Компоненты WorksPad и их назначение

WorksPad состоит из следующих компонентов – сервисов:

- **Gateway Service** – сервис, принимающий информацию от клиентских приложений и веб-приложений WorksPad. Работает по протоколам HTTPS, WSS и TCP. Основными задачами данного сервиса являются:
    - Первичная аутентификация пользователя;
    - Регистрация пользовательских устройств;
    - Выполнение операций над файлами и папками (Общие папки SMB, библиотеки документов SharePoint, Папки WebDAV);
    - Выполнение операций над сообщениями электронной почты, контактами, календарными событиями и другой почтовой функциональностью;
    - Обеспечение взаимодействия пользователей с чат-ботами;
    - Обработка запросов от веб-браузеров клиентских приложений WorksPad;
    - Журналирование запросов пользователей.
- **Share Service** – сервис, который предназначен для выполнения операций над внешними ссылками. Получает запросы от Gateway и Сайта внешнего доступа по протоколу HTTPS. Также сервис отправляет запросы на Gateway.
- **Notification Service** – сервис, который предназначен для отправки push-уведомлений клиентским приложениям WorksPad, а также для отправки служебных уведомлений администраторам системы WorksPad. Работает по протоколу HTTPS.
- **Archiver Service** – сервис, который занимается архивированием журнала событий сервера WorksPad. По умолчанию архивирование запускается каждый день в 2:00 и имеет ограничение продолжительности выполнения равное 3 часам.

Компонент **Admin API** представляет собой веб-приложение, которое позволяет управлять системой WorksPad посредством использования веб-API. Доступ к функциональности Admin API имеют пользователи с системной ролью «Администратор» или с какой-либо пользовательской ролью администрирования в системе WorksPad.

Компонент **Chatbot API** представляет собой веб-приложение, которое позволяет чат-ботам взаимодействовать с пользователями WorksPad и сторонних мессенджеров (Telegram, Microsoft Teams) посредством использования веб-API.

Кроме вышеуказанных компонентов, в состав WorksPad входят веб-приложения Консоль администратора (**Administration Console)**, Пользовательский портал (**User Portal)** и Сайт внешнего доступа (**External Access Site)**. Доступ к веб-приложениям Консоль администратора и Пользовательский портал регулируется ролями WorksPad: к Консоли администратора имеют доступ только пользователи с системной ролью «Администратор» или с какой-либо пользовательской ролью администрирования в системе WorksPad. Соответственно к пользовательскому порталу имеют доступ только пользователи с системной ролью «Пользователь». Пользователи WorksPad могут владеть несколькими ролями одновременно.

3. Управление лицензиями

Управление лицензиями WorksPad осуществляется при помощи лицензионных файлов с расширением **.lic**.

Просмотреть параметры текущей лицензии, а также загрузить новую лицензию можно при помощи Консоли администратора в разделе «Информация». Подробнее см. Руководство администратора.

4. Системные требования

Компоненты сервера WorksPad функционируют под управлением ОС **Debian 9, Astra Linux 2.12, 1.7.1 или более поздней версии**. На всех серверах должен быть развернут **Microsoft ASP.NET Core 5.0** и плагин **GSS-NTMLSSP**.

Для хранения служебной информации WorksPad использует **PostgreSQL 11 или более поздней версии**.

Для работы с общими папками SMB, WorksPad использует протокол **SMB версий 2.0.2, 2.1.0 и 3.0.0**.

Для работы с библиотеками документов SharePoint (SharePoint Document Libraries), WorksPad требует наличия **Microsoft SharePoint Server 2010 или более поздней версии**.

Для работы почтовой функциональности, WorksPad поддерживает следующие типы почтовых серверов:

- **RuPost**
- **Zimbra 8.8 или более поздней версии;**
- **Microsoft Exchange Server 2010 SP1 или более поздней версии**;
- **CommuniGate Pro 6.0 или более поздней версии**.

Система WorksPad поддерживает интеграцию с DLP-системой **InfoWatch Traffic Monitor 6.5 или более поздней версии**.

Аутентификация пользователей WorksPad осуществляется при помощи **LDAP** (Microsoft Active Directory, ALD Pro, FreeIPA, OpenLDAP).

Требования к объему оперативной памяти и дисковому пространству зависят от варианта развертывания и ожидаемого числа пользователей. Подробнее о вариантах конфигурации см. раздел Варианты топологии системы.

Ниже приведены минимальные системные требования при развёртывании всех компонентов WorksPad на одном сервере и для обслуживания до 200 пользователей**:**
Процессор: 4-ядерный,
Оперативная память: 8 ГБ,
Дисковое пространство: 1 ГБ (без учета объема пользовательских и опубликованных файлов).

5. Варианты топологии системы

5.1. Односерверная топология

С точки зрения безопасности рекомендуется разворачивать систему во внутренней сети организации. Разместите обратный прокси-сервер на одном компьютере с сервером WorksPad. Это позволит уменьшить количество публикуемых сетевых портов, а также предоставит администратору более широкие возможности по настройке сетевого взаимодействия. Подробнее см. раздел Установка и настройка обратного прокси-сервера.

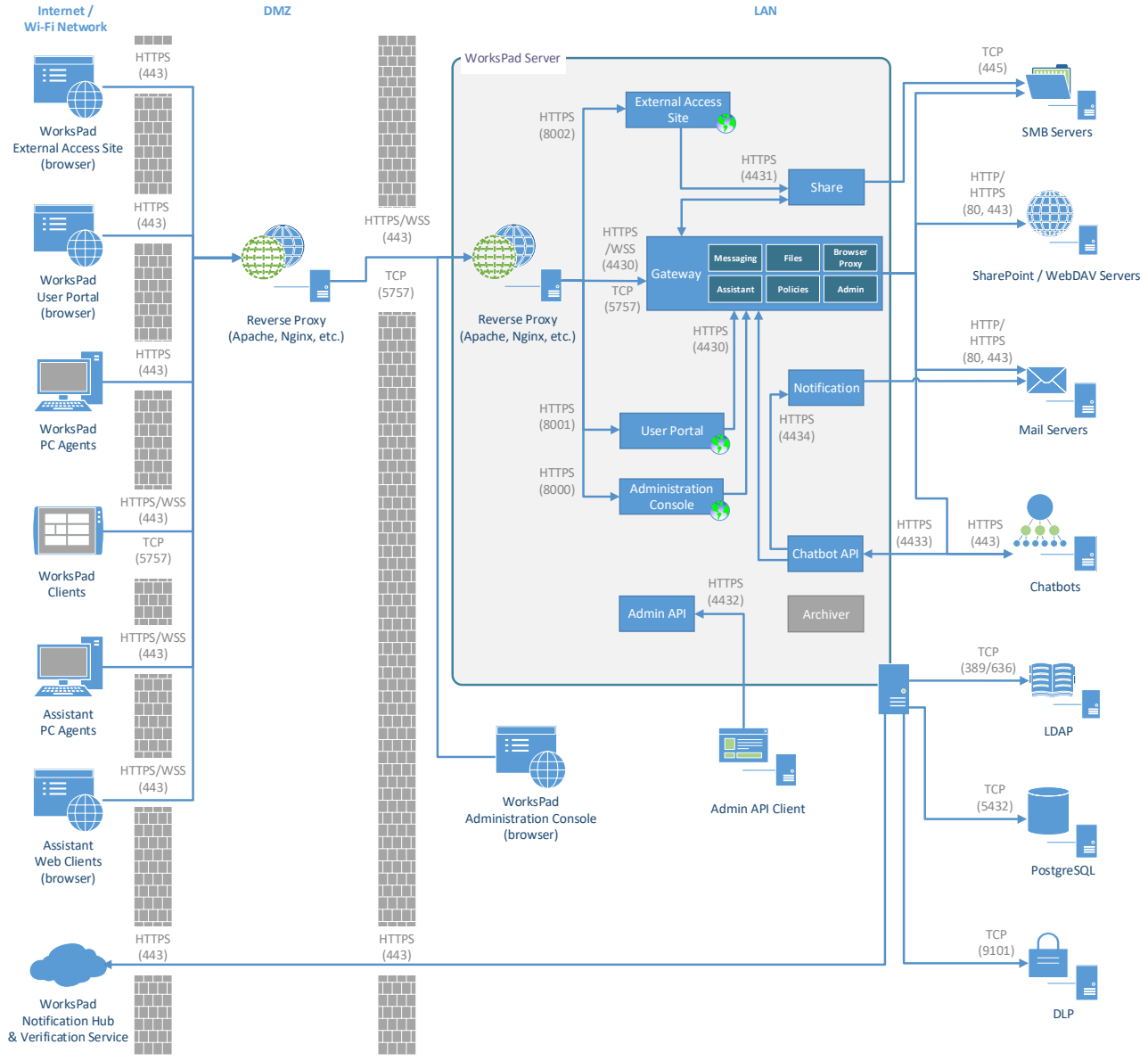


Диаграмма 1. Пример односерверной конфигурации WorksPad.

Для доступа к системе из Интернета можно воспользоваться существующим прокси-сервером в DMZ или VPN-подключением, если таковые имеются.

Доступ к Консоли администратора, Admin API и Chatbot API рекомендуется предоставлять только из внутренней сети организации.

5.2. Многосерверная топология

Для обслуживания большого количества пользователей рекомендуется использовать кластер серверов WorksPad. Использование кластера позволяет легко масштабировать систему, балансировать нагрузку, а также повышает её отказоустойчивость.

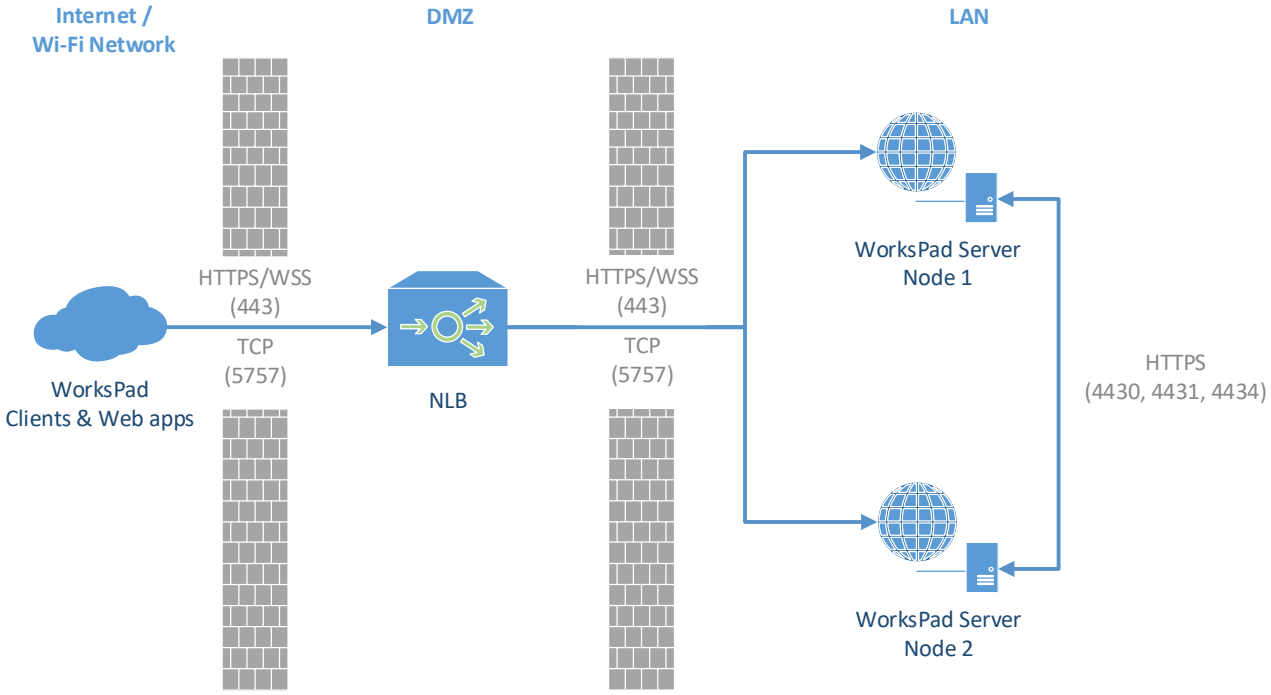


Диаграмма 2. Пример кластера WorksPad из двух узлов.

В качестве входной точки для клиентских приложений WorksPad необходимо использовать адрес аппаратного или программного балансировщика нагрузки (NLB), который будет распределять запросы между узлами кластера.

Все узлы кластера WorksPad должны использовать единую базу данных. Рекомендуется использовать кластер PostgreSQL.

Убедитесь, что со всех узлов кластера доступны ресурсы организации (файловые хранилища, почтовые сервера и т.д.), интегрированные с сервером WorksPad.

6. Подготовка инфраструктуры

Подготовка инфраструктуры включает в себя следующие шаги:

- Установка серверов (аппаратных или виртуальных) с ОС Debian 9 или более поздних версий.
- Установка Microsoft ASP.NET Core 5.0 на всех серверах, где планируется использовать компоненты WorksPad.
- Установка плагина GSS-NTLMSSP.
- Развертывание и настройка PostgreSQL 11 или более поздней версии.
- Установка и настройка обратного прокси-сервера.
- Настройка интеграции с Microsoft Exchange, если требуется.
- Настройка интеграции с CommuniGate Pro, если требуется.
- Настройка интеграции с Microsoft SharePoint, если требуется.
- Настройка интеграции с InfoWatch Traffic Monitor, если требуется.
- Настройка сетевых портов для всех серверов, в тех случаях, когда этого требует текущая инфраструктура. Подробнее см. раздел Рекомендованная конфигурация портов.

6.1. Установка Microsoft ASP.NET Core

Все компоненты WorksPad работают в среде выполнения ASP.NET Core версии 5.0.

Для установки пакета необходимо выполнить в терминале указанные ниже команды.

6.1.1. Debian 11

```
wget https://packages.microsoft.com/config/debian/11/packages-microsoft-prod.deb -O packages-microsoft-prod.deb
sudo dpkg -i packages-microsoft-prod.deb
rm packages-microsoft-prod.deb

sudo apt-get update; \
  sudo apt-get install -y aspnetcore-runtime-5.0 apt-transport-https
```

6.1.2. Debian 10 и Astra Linux 1.7.1

```
wget https://packages.microsoft.com/config/debian/10/packages-microsoft-prod.deb -O packages-microsoft-prod.deb
sudo dpkg -i packages-microsoft-prod.deb
rm packages-microsoft-prod.deb

sudo apt-get update; \
  sudo apt-get install -y aspnetcore-runtime-5.0 apt-transport-https
```

6.1.3. Debian 9 и Astra Linux 2.12

```
wget -O - https://packages.microsoft.com/keys/microsoft.asc | gpg --dearmor > microsoft.asc.gpg
sudo mv microsoft.asc.gpg /etc/apt/trusted.gpg.d/
wget https://packages.microsoft.com/config/debian/9/prod.list
sudo mv prod.list /etc/apt/sources.list.d/microsoft-prod.list
sudo chown root:root /etc/apt/trusted.gpg.d/microsoft.asc.gpg
```

```
sudo chown root:root /etc/apt/sources.list.d/microsoft-prod.list

sudo apt-get update; \
  sudo apt-get install -y apt-transport-https && \
  sudo apt-get update && \
  sudo apt-get install -y aspnetcore-runtime-5.0
```

6.2. Установка GSS-NTLMSSP

GSS-NTLMSSP – это плагин механизма GSSAPI, реализующий NTLM-аутентификацию. Используется сервером WorksPad при взаимодействии с почтовыми системами и файловыми источниками.

Для установки пакета необходимо выполнить в терминале указанную ниже команду:

```
sudo apt-get install gss-ntlmssp
```

6.3. Установка PostgreSQL

Для работы сервера WorksPad требуется PostgreSQL 11 или более поздней версии.

SQL сервер допустимо размещать локально, на том же сервере, где расположены компоненты сервера WorksPad. Более сложный варианты топологии, например, множественная установка компонентов с использованием балансировки нагрузки, может потребовать выделения отдельного сервера (отказоустойчивого кластера) для размещения базы данных.

Для установки пакета необходимо выполнить в терминале указанную ниже команду:

```
sudo apt-get install postgresql-11
```

6.4. Установка и настройка обратного прокси-сервера

Каждый компонент сервера WorksPad, который имеет интерфейс для сетевого взаимодействия, использует отдельный сетевой порт. Данные компоненты работают под управлением кроссплатформенного веб-сервера Microsoft Kestrel.

Вместе с веб-сервером Kestrel рекомендуется использовать обратный прокси-сервер (Nginx, Apache и т.п.). Это позволит уменьшить количество публикуемых сетевых портов в Интернет, а также предоставит администратору более широкие возможности по настройке сетевого взаимодействия.

Обратный прокси-сервер можно разместить на отдельном компьютере или на одном компьютере с сервером WorksPad.

В рамках данного руководства в качестве обратного прокси-сервера рассматривается Nginx. Рекомендуется использовать версию 1.15.6 или выше.

Установите Nginx в соответствии с версией Вашего сервера Linux. Инструкции по установке для различных версий Linux доступны на официальном сайте Nginx: https://nginx.org/ru/linux_packages.html.

Поместите файл, представленный в разделе Приложение 1, в папку с включёнными сайтами Nginx. В большинстве случаев это либо «/etc/nginx/sites-enabled/», либо «/etc/nginx/conf.d/». Уточнить, какую папку использует Nginx, можно в файле «/etc/nginx/nginx.conf», директива «include» в секции «http».

6.5. Настройка интеграции с Microsoft Exchange

Данный этап необходим, если для обеспечения почтовой функциональности системы WorksPad планируется использовать почтовый сервер Microsoft Exchange или почтовые службы Office 365. В противном случае можете пропустить этот шаг.

6.5.1. Настройка политики регулирования Microsoft Exchange

Внимание! Администратор не может устанавливать политики регулирования для Office 365.

Для работы WorksPad с сервером Exchange рекомендуется снять ограничения, накладываемые политикой регулирования клиентов Microsoft Exchange по умолчанию. В противном случае, в связи с довольно низкими порогами политик установленных по умолчанию для Exchange Web Services, возможны временные отказы в обслуживании запросов (или более медленное их обслуживание) со стороны Exchange Server. Вероятность срабатывания политик высока для ящиков больших размеров, особенно при первоначальной синхронизации.

Ниже представлено описание шагов, которые необходимо выполнить администратору для снятия ограничений в зависимости от версии Exchange.

6.5.1.1. *Настройка политики регулирования для Microsoft Exchange 2010*

Для настройки политики регулирования клиентов на Microsoft Exchange 2010 необходимо выполнить следующие шаги:

1. Войти на Exchange Server от имени учётной записи администратора и запустить Exchange Management Shell
2. Для создания новой политики регулирования, необходимо выполнить следующую команду:
   ```
   New-ThrottlingPolicy WorksPadPolicy -EWSMaxConcurrency $null -
   EWSPercentTimeInAD $null -EWSPercentTimeInCAS $null -
   EWSPercentTimeInMailboxRPC $null -EWSMaxSubscriptions $null -
   EWSFastSearchTimeoutInSeconds $null -EWSFindCountLimit $null
   ```
3. Выполните следующую команду для применения новой политики ко всем владельцам почтовых ящиков, к которым обращаются пользователи WorksPad:
   ```
   Set-Mailbox "<user login>" -ThrottlingPolicy WorksPadPolicy
   ```
4. Для применения новой политики к системной учётной записи для push-уведомлений выполните следующую команду:
   ```
   Set-ThrottlingPolicyAssociation -Identity "<user login>" -
   ThrottlingPolicy WorksPadPolicy
   ```

6.5.1.2. *Настройка политики регулирования для Microsoft Exchange 2013 и выше*

Для настройки политики регулирования клиентов на Microsoft Exchange 2013 и выше необходимо выполнить следующие шаги:

1. Войдите на сервер где установлен Microsoft Exchange Server от имени учётной записи администратора и запустить Exchange Management Shell

2. Для создания новой политики регулирования, необходимо выполнить следующую команду:
   `New-ThrottlingPolicy **WorksPadPolicy** -RCAMaxConcurrency Unlimited -EWSMaxConcurrency Unlimited -EWSMaxSubscriptions Unlimited -CPAMaxConcurrency Unlimited -EwsCutoffBalance Unlimited -EwsMaxBurst Unlimited -EwsRechargeRate Unlimited`
3. Выполните следующую команду для применения новой политики ко всем владельцам почтовых ящиков, к которым обращаются пользователи WorksPad:
   `Set-Mailbox "<user login>" -ThrottlingPolicy **WorksPadPolicy**`
4. Для применения новой политики к системной учётной записи для push-уведомлений выполните следующую команду:
   `Set-ThrottlingPolicyAssociation -Identity "<user login>" -ThrottlingPolicy **WorksPadPolicy**`

6.5.2. Настройка Autodiscover

Данный этап необходим, если планируется использовать push-уведомления о почтовых событиях в клиентских приложениях WorksPad. В противном случае можете пропустить этот шаг.

Автообнаружение (Autodiscover) используется для определения связей между CAS (Client Access Server) и адресами электронной почты. Это является необходимым требованием для корректной работы почтовых уведомлений.

Необходимо чтобы служба автообнаружения Exchange была доступна с сервера, где развёрнута служба WorksPad Notification Service.

6.5.3. Создание системной учётной записи для почтовых push-уведомлений

Данный этап необходим, если планируется использовать push-уведомления о почтовых событиях в клиентских приложениях WorksPad. В противном случае можете пропустить этот шаг.

Для получения и обработки почтовых уведомлений от сервера Exchange необходимо иметь системную учётную запись с правами на олицетворение (роль ApplicationImpersonation) в Microsoft Exchange. Данная учётная запись позволяет создавать от имени пользователя подписки на получение почтовых уведомлений от Exchange, а также получать необходимую для отправки push-уведомлений информацию.

Создайте системную учётную запись, например, «WPNotification». Учётной записи рекомендуется задать надёжный пароль. **Срок действия пароля должен быть не ограничен**. **Имя** и **пароль** этой учетной записи должны оставаться **неизменными**.

Далее представлено описание шагов, которые необходимо выполнить администратору Microsoft Exchange для предоставления необходимых прав системной учётной записи:

1. Войдите на сервер Microsoft Exchange Server от имени учётной записи администратора и запустите Exchange Management Shell
2. Для предоставления системной учётной записи прав на олицетворение выполните следующую команду:
   `New-ManagementRoleAssignment -Name **"WorksPad Notification Admin"** -Role:ApplicationImpersonation -User "<user login>"`

Внимание! Для данной системной учётной записи крайне рекомендуется снять ограничения, накладываемые политикой регулирования клиентов Microsoft Exchange по умолчанию (не применимо к Office 365). Подробнее см. раздел «Настройка политики регулирования Microsoft Exchange».

6.6. Настройка интеграции с CommuniGate Pro

Данный этап необходим, если для обеспечения почтовой функциональности системы WorksPad планируется использовать почтовый сервер CommuniGate Pro. В противном случае можете пропустить этот шаг.

6.6.1. Установка скриптов и настройка правил для входящей почты

Данный этап необходим, если планируется использовать push-уведомления о почтовых событиях в клиентских приложениях WorksPad. В противном случае можете пропустить этот шаг.

Для получения и обработки почтовых уведомлений от сервера CommuniGate Pro необходимо установить специальные скрипты из пакета WorksPad CGP Push Sender[1], а также настроить правила для входящей почты.

Примечание. Правила для входящей почты должны быть настроены для всех доменов, пользователи которых добавлены в систему WorksPad.

Перед установкой скрипта «workspad-pushhandler.sppr» из пакета WorksPad CGP Push Sender необходимо его подготовить. Для этого выполните указанные ниже действия:

1. Откройте на редактирование файл «workspad-pushhandler.sppr».
2. Укажите в файле URL-адрес службы WorksPad Notification Service, отредактировав указанный в нём шаблон «https://<WorksPadServer>/Notification/SendCgpPush» (например, «https://192.168.10.10/Notification/SendCgpPush»).
   Примечание. Обратите внимание, что CommuniGate Pro поддерживает взаимодействие по протоколу HTTPS из скрипта только с использованием стандартного порта 443. В связи с этим необходимо опубликовать службу Notification Service по адресу «https://<WorksPadServer>/Notification» с использованием обратного прокси-сервера.
3. Сохраните файл.

Далее представлено описание шагов, которые необходимо выполнить администратору CommuniGate Pro для установки скриптов и настройки правил для входящей почты:

1. Войдите в интерфейс Администратора CommuniGate Pro от имени учётной записи администратора.
2. Перейдите в раздел «Пользователи» – «Интерфейсы».
3. На открывшейся странице загрузите файл «workspad-pushsender.wcgp».
4. Перейдите в раздел «Пользователи» – «PBX».
5. На открывшейся странице загрузите файл «workspad-pushhandler.sppr».
6. Перейдите в раздел «Пользователи» – «Домены».

[1] Для получения пакета свяжитесь с Вашим поставщиком решения WorksPad.

7. В представленной таблице нажмите на имя домена, в котором необходимо настроить правила входящей почты.
8. Перейдите в раздел «Почта» выбранного домена.
9. На открывшейся странице создайте следующее правило:

Приоритет	**Имя**	
7	PushMail	
Данные	**Операция**	**Параметр**
-	-	-
Действие	**Параметр**	
Обратиться по URL	http://127.0.0.1:8100/sys/workspad-pushsender.wcgp?type=mailIn&sub=^s&fromFull=^F&from=^E&to=^R&rcpt=^r&messageId=^I	

6.6.2. Создание системной учётной записи для почтовых push-уведомлений

Данный этап необходим, если планируется использовать push-уведомления о почтовых событиях в клиентских приложениях WorksPad. В противном случае можете пропустить этот шаг.

Для получения и обработки почтовых уведомлений от сервера CommuniGate Pro необходимо иметь системную учётную запись с правом доступа «**Полный доступ ко всем Папкам**». Данная учётная запись позволяет получать необходимую для отправки push-уведомлений информацию.

Примечание. Система WorksPad не использует системную учётную запись для изменения настроек сервера CommuniGate Pro и данных её пользователей. Предоставленные права доступа используются только для получения информации о новых входящих сообщениях, которая необходима для работы push-уведомлений.

Создайте системную учётную запись, например, «WPNotification». Учётной записи рекомендуется задать надёжный пароль. **Срок действия пароля должен быть не ограничен**. **Имя** и **пароль** этой учетной записи должны оставаться **неизменными**.

Далее представлено описание шагов, которые необходимо выполнить администратору CommuniGate Pro для предоставления необходимых прав системной учётной записи:

1. Войдите в интерфейс Администратора CommuniGate Pro от имени учётной записи администратора.
2. Перейдите в раздел «Пользователи» – «Домены» и в представленной там таблице нажмите на имя домена, в котором была создана системная учётная запись для работы функциональности push-уведомлений.
3. В открывшемся разделе «Объекты» нажмите на имя системной учётной записи пользователя.
4. Нажмите на ссылку «Права Доступа», которая расположена в правом верхнем углу открывшейся страницы.
5. Выберите для пользователя следующие группу прав доступа – «**Может менять установки Всех Доменов и Пользователей**».
6. В разделе «**Объекты**» укажите право доступа – «**Полный доступ ко всем Папкам**».

7. Нажмите кнопку «Модифицировать».

6.7. Настройка интеграции с Microsoft SharePoint

Данный этап необходим, если с помощью системы WorksPad планируется обеспечить доступ к библиотекам документов Microsoft SharePoint или SharePoint Online. В противном случае можете пропустить этот шаг.

Для доступа к документам, размещенным на порталах Microsoft SharePoint пользователи должны обладать соответствующими правами. Следующие разрешения должны быть предоставлены пользователям на каждом портале SharePoint в зависимости от желаемого режима доступа:

Режим	Описание режима	Разрешения SharePoint
«Чтение»	Чтение и скачивание документов на мобильное устройство	View Items, Browse Directories, View Pages, Use Remote Interfaces, Open
«Совместная работа»	«Чтение» + Загрузка документов: добавление с возможностью замены без удаления	+ Add Items, Edit Items
«Редактирование»	«Совместная работа» + Удаление	+ Delete Items

6.8. Настройка интеграции с InfoWatch Traffic Monitor

Данный этап необходим, если планируется интеграция системы WorksPad с DLP-системой InfoWatch Traffic Monitor (IWTM). В противном случае можете пропустить этот шаг.

В рамках интеграции с DLP-системой, сервер WorksPad отправляет теневые копии файлов, скачиваемых на мобильные устройства, на сервер IWTM. Для настройки взаимодействия сервера WorksPad с DLP-системой IWTM необходимо установить плагин WorksPad TM Adapter[2] в систему IWTM. Подробнее об интеграции WorksPad с DLP-системой смотрите в «Руководстве по интеграции с InfoWatch Traffic Monitor».

6.9. Рекомендованная конфигурация портов

Для работы компонентов WorksPad необходимо открыть ряд сетевых портов из внешних сетей к серверу WorksPad, от сервера WorksPad к внутренним ресурсам и системам (серверу БД, контроллерам домена, почтовым серверам и пр.). Также для работы некоторых компонентов системы может потребоваться открытие сетевых портов от серверов WorksPad в Интернет. В таблице ниже представлен перечень необходимых портов с указанием компонентов WorksPad и внешних систем.

Порт	Протокол	Источник	Точка обращения
443	HTTPS, WSS	Интернет, интранет	Reverse Proxy
5757	TCP	Интернет, интранет	Reverse Proxy

[2] Для получения плагина свяжитесь с Вашим поставщиком решения WorksPad.

8000	HTTPS	Reverse Proxy	Administration Console
8001	HTTPS	Reverse Proxy	User Portal
8002	HTTPS	Reverse Proxy	External Access Site
4430	HTTPS, WSS	Reverse Proxy	Gateway Service
5757	TCP	Reverse Proxy	Gateway Service
4432	HTTPS	Reverse Proxy	Admin API
4434*	HTTPS	Reverse Proxy	Notification Service
4430	HTTPS	Administration Console	Gateway Service
4430	HTTPS	User Portal	Gateway Service
4431	HTTPS	External Access Site	Share Service
4431	HTTPS	Gateway Service	Share Service
4430	HTTPS	Share Service	Gateway Service
80, 443	HTTP, HTTPS	Gateway Service	Серверы Microsoft SharePoint
80, 443	WebDAV	Gateway Service	Серверы WebDAV
445	SMB	Gateway Service	Файловые серверы (SMB)
993	IMAP	Gateway Service	Почтовые серверы RuPost
465	SMTP	Gateway Service	Почтовые серверы RuPost
443	CalDAV, CardDAV	Gateway Service	Почтовые серверы RuPost
143	IMAP	Gateway Service	Почтовые серверы Zimbra
587	SMTP	Gateway Service	Почтовые серверы Zimbra
443	CalDAV, CardDAV	Gateway Service	Почтовые серверы Zimbra
80, 443	HTTP, HTTPS	Gateway Service, Notification Service	Почтовые серверы Microsoft Exchange
8100, 9100	HTTP, HTTPS	Gateway Service, Notification Service	Почтовые серверы CommuniGate Pro
443*	HTTPS	Почтовый сервер CommuniGate Pro	Reverse Proxy
9101	TCP	Gateway Service	DLP-система InfoWatch Traffic Monitor
443	HTTPS	Gateway Service, Chatbot API	Чат-боты
4430	HTTPS	Chatbot API	Gateway Service
4434	HTTPS	Chatbot API	Notification Service

4433	HTTPS	Чат-боты	Chatbot API
5432	TCP	Gateway Service, Notification Service, Share Service, Archiver Service, Admin API, Chatbot API	PostgreSQL
389, 636	TCP	Gateway Service, Admin API	Контроллер домена (LDAP)
80, 443**	TCP	Gateway Service	Интернет, интранет
443***	HTTPS	Gateway Service, Admin API	Интернет (WorksPad Verification Service)
443****	HTTPS	Notification Service	Интернет (WorksPad Notification Hub)

* Необходимо для работы push-уведомлений о почтовых событиях с сервера CommuniGate Pro.
** Порты и IP-адреса устанавливаются в зависимости от расположения веб-ресурсов, к которым необходимо предоставить доступ через встроенный веб-браузер WorksPad.
*** Необходимо для активации лицензий. Сервер WorksPad Verification Service: ivs.workspad.com.
****Необходимо для работы push-уведомлений. Серверы назначения зависят от выбранного региона расположения сервиса уведомлений WorksPad Notification Hub (настраивается в Консоли администратора). Серверы WorksPad Notification Hub в регионе «Европа»: push-eu-01p.workspad.com, push-eu-02p.workspad.com.

Следует обратить внимание, что в таблице описаны порты, требующиеся для работы непосредственно компонентов WorksPad, однако, для взаимодействия серверов, являющихся членами домена LDAP, может потребоваться настройка и других сетевых портов/протоколов. Например, tcp/135, tcp/137, tcp/3268, tcp/3269, tcp/42, tcp/445, tcp/464, tcp/49152-65535, tcp/88, tcp/ldap, tcp/ldaps, tcp/netbios-ssn, udp/389, udp/445, udp/464, udp/88, udp/domain, udp/nameserver, udp/netbios-dgm, udp/netbios-ns, udp/ntp.

Подробное рассмотрение сетевого взаимодействия между серверами в инфраструктуре домена LDAP выходит за рамки данного руководства.

7. Действия перед началом установки

Перед установкой системы WorksPad необходимо предварительно выполнить следующие действия:

- Создать базу данных в PostgreSQL.
- Создать корневую папку для клиентских журналов событий, если планируется использовать хранилище клиентских журналов событий.
- Создать корневую папку для FileBox, если планируется использовать WorksPad FileBox.
- Создать корневую папку для опубликованных файлов, если планируется использовать функциональность внешних ссылок.

7.1. Создание базы данных в PostgreSQL

Необходимо предварительно создать пустую базу данных в PostgreSQL. Во время первой установки туда будут добавлены все необходимые компоненты базы данных для системы WorksPad. Рекомендуемое название базы данных – «WorksPad». Также рекомендуется создать в PostgreSQL специального пользователя «workspad» и предоставить ему полные права на базу данных WorksPad.

7.2. Создание корневой папки для клиентских журналов событий

Данные действия необходимо выполнить, только если планируется использование хранилища клиентских журналов событий WorksPad.

Создайте сетевую папку SMB – корневой путь к клиентским журналам событий. В этой папке в последующем будут сохраняться клиентские журналы событий, отправленные пользователями на сервер из клиентских приложений WorksPad. В качестве имени для папки можно использовать, например, «WorksPadClientLogs». На папку необходимо предоставить **полные права доступа** пользователю, который в последующем будет использоваться для взаимодействия с данной папкой.

7.3. Создание корневой папки для FileBox

Данные действия необходимо выполнить, только если планируется использование WorksPad FileBox.

Создайте общую папку SMB – **корневой путь к пользовательским папкам**. В этой папке в последующем будут создаваться персональные папки пользователей WorksPad. В качестве имени для папки можно использовать, например, «WorksPadFileBox». На данную папку необходимо предоставить **полные права доступа пользователям всех доменов** (группы «Domain Users» всех доменов, пользователи которых будут работать с системой WorksPad).

7.4. Создание корневой папки для опубликованных файлов

Данные действия необходимо выполнить, только если планируется использование функциональности внешних ссылок WorksPad.

Создайте общую папку SMB – **корневой путь к опубликованным файлам**. В этой папке в последующем будут размещены опубликованные по внешним ссылкам файлы. В качестве имени для папки можно использовать, например, «WorksPadShareBox». На папку необходимо предоставить **полные права доступа** пользователю, который в последующем будет использоваться для взаимодействия с данной папкой.

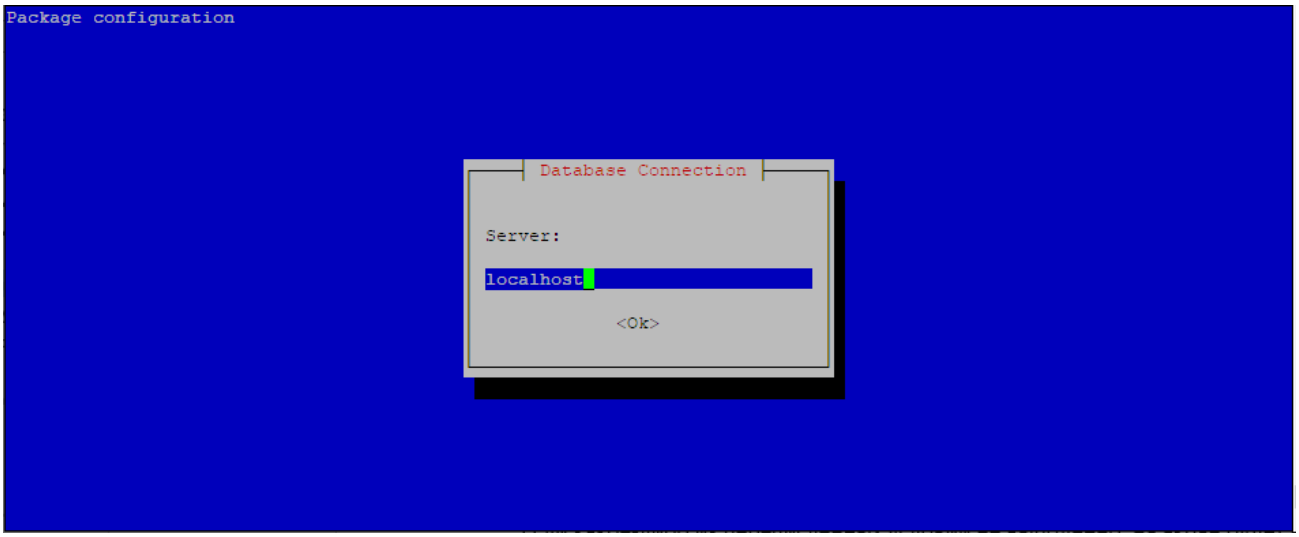
8. Установка системы

Для установки пакета WorksPad необходимо выполнить в терминале указанную ниже команду:

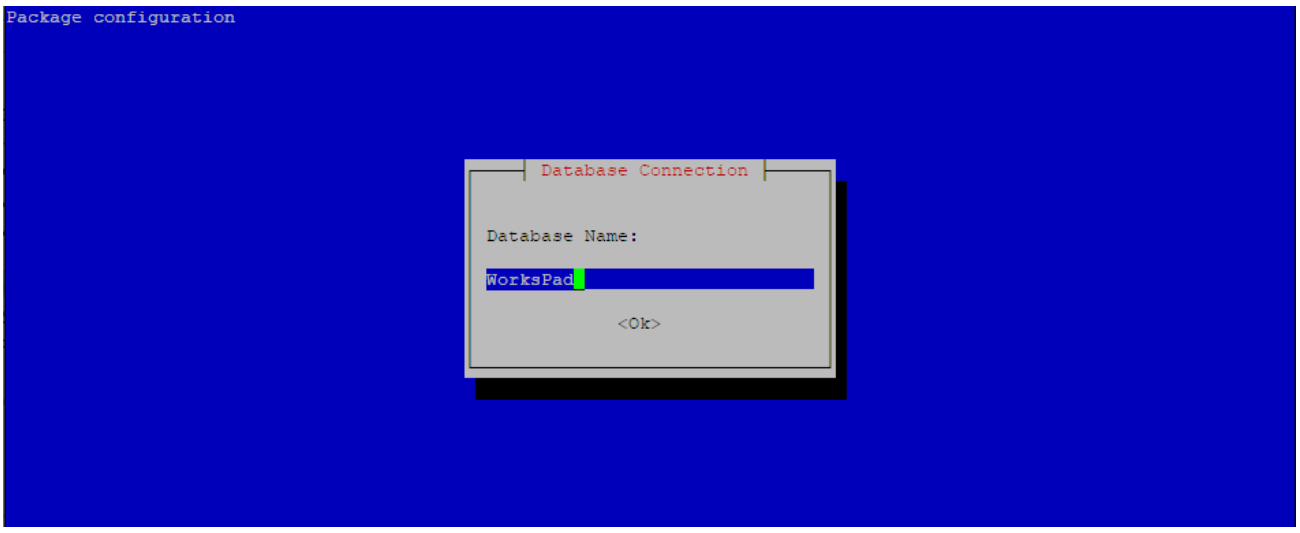
```
sudo dpkg -i /tmp/workspad_amd64.deb
```

Программа установки выполнена в виде мастера. Рассмотрим подробно каждый шаг процедуры установки пакета.

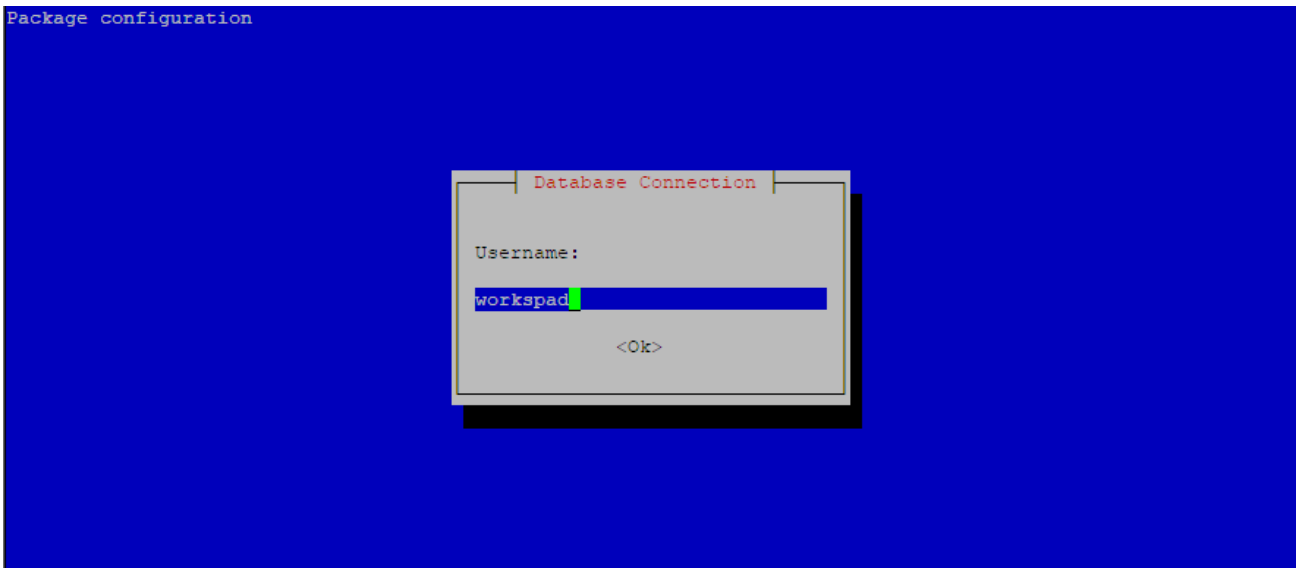
Шаг 1. Необходимо указать название сервера базы данных. При необходимости можно задать нестандартный порт, указав сервер баз данных в следующем формате: «<hostname>:<port>».



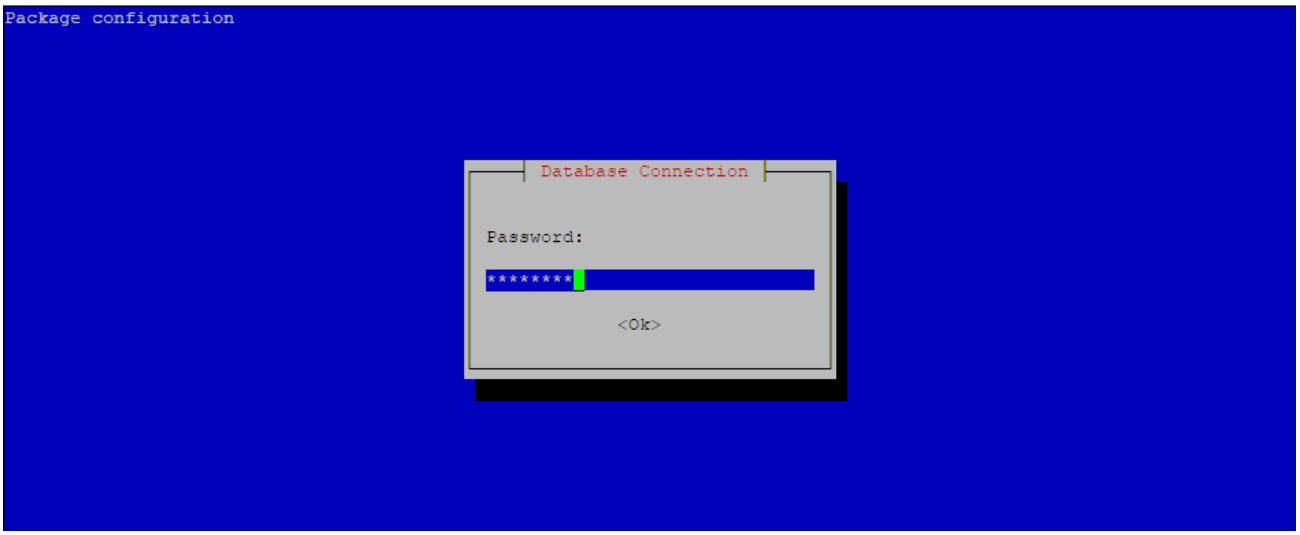
Шаг 2. Необходимо указать название базы данных.



Шаг 3. Необходимо указать имя пользователя для доступа к базе данных.



Шаг 4. Необходимо указать пароль, соответствующий пользователю из предыдущего шага.



Если все параметры были указаны верно, то установка сервера WorksPad завершится успешно.

В следующем разделе подробно описаны параметры установленной системы.

8.1. Параметры установленной системы

Компоненты сервера WorksPad устанавливаются в директорию «/opt/workspad».

В результате установки сервера, в systemd регистрируются указанные ниже службы.

Служба в systemd	Компонент сервера WorksPad
workspad-adminapi.service	Admin API
workspad-adminportal.service	Administration Console
workspad-archiver.service	Archiver Service

workspad-chatbotapi.service	Chatbot API
workspad-externalportal.service	External Access Site
workspad-gateway.service	Gateway Service
workspad-notification.service	Notification Service
workspad-share.service	Share Service
workspad-userportal.service	User Portal

Службы работают от имени специально созданной служебной учётной записи «workspad».

Во время первой установки сервера WorksPad создаётся специальный **сертификат безопасности**. Он служит для обеспечения конфиденциальности информации, хранимой в системе. В случае использования кластера серверов WorksPad, данный сертификат необходимо самостоятельно установить на другие сервера. Подробнее см. раздел Создание кластера WorksPad.

8.2. Первоначальная настройка системы

Для первоначальной настройки системы WorksPad используется специальная учётная запись «**local\admin**» (локальный администратор). Пароль по умолчанию «**wpAdmin123**». Используйте её для входа в Консоль администратор сразу после установки системы.

Используя данную учётную запись зарегистрируйте в системе первый домен (LDAP). После этого добавьте в систему одного из пользователей этого домена, назначив ему роль «Администратор». Дальнейшую настройку системы производите от имени добавленного пользователя. Отключите учётную запись локального администратора. Подробнее см. раздел Настройка локального администратора.

Рекомендуется изменить SSL-сертификат, используемый по умолчанию для Browser Proxy, на действительный сертификат для Вашего домена, выпущенный доверенным центром сертификации. Подробнее см. раздел Настройка Browser Proxy. Этот же сертификат используйте на обратном прокси-сервере. Подробнее см. раздел Приложение 1.

Установите лицензию WorksPad используя Консоль администратора. Подробнее см. Руководство администратора.

9. Создание кластера WorksPad

Подробное описание кластера WorksPad представлено в разделе Многосерверная топология.

При установке нового узла WorksPad укажите базу данных, которую использовали при первом развёртывании системы.

Между всеми узлами системы необходимо открыть доступ по портам: **4430, 4431** и **4434**. Данные порты используются для взаимодействия компонентов сервера WorksPad между собой.

На всех узлах кластера должен быть развёрнут сертификат безопасности. Он автоматически создаётся при первом развёртывании системы. Для добавления сертификата на новый узел необходимо выполнить следующие действия:

1. Выполните экспорт сертификата безопасности на первом узле WorksPad. Для этого в терминале первого узла выполните указанную ниже команду:
   `sudo -u workspad /usr/bin/dotnet /opt/workspad/CertTool/WorksPadCertTool.dll export --t <thumbprint> --f /tmp/sec_cert.pfx --p <password>`
   Замените **<thumbprint>** на хэш сертификата безопасности. Его можно посмотреть в Консоли администратора в разделе «Общие настройки» (подробнее см. Руководство администратора).
   Замените **<password>** на пароль, которым будет защищён файл сертификата.
   Внимание! Команду необходимо выполнять от имени пользователя «workspad».
2. Скопируйте файл сертификата безопасности «/tmp/sec_cert.pfx» на сервер нового узла WorksPad в папку «/tmp».
3. Добавьте сертификат безопасности в хранилище сертификатов нового узла. Для этого в терминале нового узла выполните указанную ниже команду:
   `sudo -u workspad /usr/bin/dotnet /opt/workspad/CertTool/WorksPadCertTool.dll addseccert --f /tmp/sec_cert.pfx --p <password>`
   Замените **<password>** на пароль, которым защищён файл сертификата.
   Внимание! Команду необходимо выполнять от имени пользователя «workspad».

После установки нового узла WorksPad, его компоненты автоматически зарегистрируют себя в системе.

Подключите новый узел к балансировщику нагрузки для обработки **HTTPS/WSS** трафика по порту **443** и **TCP** трафика по порту **5757**.

На балансировщике нагрузки используйте действительный сертификат для Вашего домена, выпущенный доверенным центром сертификации.

Балансировщик нагрузки необходимо использовать в режиме сохранения сессии (session persistence). Например, на основе IP-адреса источника.

10. Конфигурирование системы

После установки системы WorksPad, некоторые компоненты системы можно настроить вручную, изменяя их параметры в соответствии с Вашими требованиями. Ниже представлено описание по настройке каждого из этих компонентов.

10.1. Конфигурирование Gateway Service

Чтобы произвести настройку Gateway Service необходимо открыть файл конфигурации службы **«/opt/workspad/GatewayService/appsettings.json»**.

Внимание! После изменения конфигурационного файла необходимо перезапустить службу в systemd.

10.1.1. Настройка локального администратора

Параметры учётной записи **локального администратора** «local\admin» расположены в секции «**LocalAdmin**» файла конфигурации.

Пример (представлена часть конфигурационного файла):

```
  "LocalAdmin": {
    "Enabled": true,
    "Password": "wpAdmin123"
  },
```

Для разрешения/запрета использования данной учётной записи измените значение параметра «**LocalAdmin/Enabled**» на true или false соответственно. Для смены пароля учётной записи измените значение параметра «**LocalAdmin/Password**» на любое необходимое.

10.1.2. Настройка Browser Proxy

Параметры Browser Proxy расположены в секции «**BrowserProxy**» файла конфигурации.

Пример (представлена часть конфигурационного файла):

```
  "BrowserProxy": {
    "Enabled": true,
    "LoggingTag": "ClientConnectionError, ClientRequestError, HttpProxyError, IOError",
    "ListenIP": "0.0.0.0",
    "ListenPort": "5757",
    "Certificate": {
      "Path": "../SslCert.pfx",
      "Password": "Wp.$$L",
      "AllowInvalid": true
    }
  },
```

Для включения/отключения данной функциональности измените значение параметра «**BrowserProxy/Enabled**» на true или false соответственно.

Для смены прослушиваемого IP-адреса измените значение параметра «**BrowserProxy/ListenIP**». Для смены прослушиваемого порта измените значение параметра «**BrowserProxy/ListenPort**».

Параметры SSL-сертификат для Browser Proxy расположены в секции «**BrowserProxy/Certificate**».

Поддерживаются различные источники сертификата:

- Файл «.pfx».
  Настраиваемые параметры:
  - «**BrowserProxy/Certificate/Path**» – путь к файлу сертификата в формате «.pfx».
  - «**BrowserProxy/Certificate/Password**» – пароль для доступа к данным сертификата.
- Файлы «.pem»/«.crt» и «.key».
  - «**BrowserProxy/Certificate/Path**» – путь к файлу в формате «.pem»/«.crt».
  - «**BrowserProxy/Certificate/KeyPath**» – путь к файлу в формате «.key».
  - «**BrowserProxy/Certificate/Password**» – пароль для доступа к данным сертификата.
- Хранилище сертификатов.
  - «**BrowserProxy/Certificate/Subject**» – имя субъекта для сертификата.
  - «**BrowserProxy/Certificate/Store**» – название хранилища сертификатов («My» – личное или «WebHosting» – размещение веб-служб).
  - «**BrowserProxy/Certificate/Location**» – название расположения хранилища («LocalMachine» – локальный компьютер или «CurrentUser» – текущий пользователь).

Для разрешения/запрета использования ненадёжного сертификата (например, самозаверенного) измените значение параметра «**BrowserProxy/Certificate/AllowInvalid**» на «true» или «false» соответственно.

10.1.3. Настройка прокси-сервера для Telegram

Параметры прокси-сервера для соединения Gateway Service с сервером Telegram расположены в секции «**Telegram**» файла конфигурации.

Пример (представлена часть конфигурационного файла):

```
"Telegram": {
  "ProxyAddress": "http://localhost:8888"
},
```

В значении параметра «**Telegram/ProxyAddress**» указывается URL-адрес прокси-сервера.

Примечание. Прокси-сервер должен работать в режиме «без аутентификации».

10.1.4. Настройка прокси-сервера для Microsoft Bot Framework

Параметры прокси-сервера для соединения Gateway Service с сервером Microsoft Bot Framework расположены в секции «**MsBotFramework**» файла конфигурации.

Пример (представлена часть конфигурационного файла):

```
"MsBotFramework": {
  "ProxyAddress": "http://localhost:8888"
},
```

В значении параметра «**MsBotFramework/ProxyAddress**» указывается URL-адрес прокси-сервера.

Примечание. Прокси-сервер должен работать в режиме «без аутентификации».

10.2. Конфигурирование Archiver Service

Чтобы произвести настройку Archiver Service необходимо открыть файл конфигурации службы **«/opt/workspad/ArchiverService/appsettings.json**».

Внимание! После изменения конфигурационного файла необходимо перезапустить службу в systemd.

Пример (представлена часть конфигурационного файла):

```
  "StartTime": "02:00",
  "MaxDuration": "3" // In hours
```

В значении параметра «**StartTime**» указывается время (в формате – «часы:минуты») запуска задачи архивирования журнала событий.

В значении параметра «**MaxDuration**» указывается максимальное время (в часах) выполнения задачи архивирования журнала событий.

11. Поддержка

В случае возникновения любых вопросов или проблем во время установки, пожалуйста, свяжитесь со службой технической поддержки WorksPad по адресу **support@workspad.com** или разместите свой запрос на веб-сайте **https://support.workspad.com**.

Приложение 1

В данном разделе представлен пример содержимого файла конфигурации сайта «workspad.conf» для веб-сервера Nginx, развёрнутого на одном компьютере с сервером WorksPad. Данный файл должен располагаться в папке для включённых сайтов в соответствии с директивой «include» в секции «http» файла настроек «/etc/nginx/nginx.conf».

В таблице ниже указаны правила маршрутизации, используемые в данном файле конфигурации.

Адрес Nginx	Адрес назначения	Компонент сервера WorksPad
https://[server]/	https://127.0.0.1:4430	Gateway Service
https://[server]/admin	https://127.0.0.1:8000	Administration Console
https://[server]/user	https://127.0.0.1:8001	User Portal
https://[server]/external	https://127.0.0.1:8002	External Access Site

В разделе «server» необходимо указать действительный SSL-сертификат для Вашего домена, выпущенный доверенным центром сертификации.

```
map $http_upgrade $connection_upgrade {
    default upgrade;
    '' close;
}

upstream gateway {
    server 127.0.0.1:4430 fail_timeout=0;
}

upstream admin {
    server 127.0.0.1:8000 fail_timeout=0;
}

upstream user {
    server 127.0.0.1:8001 fail_timeout=0;
}

upstream external {
    server 127.0.0.1:8002 fail_timeout=0;
}

server {
 listen 443 ssl;
 listen [::]:443 ssl;
 #Specify hostname here if you need SNI
 #server_name wp.contoso.com
 ssl_certificate /etc/nginx/ssl/workspad_public.pem;
 ssl_certificate_key /etc/nginx/ssl/workspad_private.pem;

 access_log /var/log/nginx/wp-access.log;
 error_log /var/log/nginx/wp-error.log;

 ssl_protocols TLSv1.2 TLSv1.3;
 ssl_prefer_server_ciphers on;
 #Legacy ciphers are commented out, if you use old devices you might need to adjust ciphers
accordingly
 #ssl_ciphers "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256
EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH EDH+aRSA RC4 !aNULL !eNULL !LOW !3DES !MD5
!EXP !PSK !SRP !DSS !RC4";
 #ssl_ciphers
TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:TLS_AES_128_CCM_8_SHA256:
```

```
TLS_AES_128_CCM_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-
GCM-SHA384:ECDHE-RSA-AEECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384;
 ssl_ciphers EECDH+AESGCM:EDH+AESGCM;
 ssl_ecdh_curve secp521r1:secp384r1;

 #Generate dhparam using open SSL and specify path here
 #openssl dhparam -out /etc/nginx/ssl/dhparam.pem 4096
 ssl_dhparam /etc/nginx/ssl/dhparam.pem;

 ssl_session_cache shared:SSL:10m;
 ssl_session_timeout 5m;
 ssl_buffer_size 4k;
 ssl_session_tickets off;

 ssl_stapling on;
 ssl_stapling_verify on;
 resolver 8.8.8.8 8.8.4.4 [2001:4860:4860::8888] [2001:4860:4860::8844];
 resolver_timeout 5s;

 location / {
   proxy_pass https://gateway;
   proxy_http_version 1.1;

   #Switch to web sockets protocol if such a request is received from the client
   proxy_set_header Upgrade $http_upgrade;
   proxy_set_header Connection $connection_upgrade;

   #Note! Nginx 1.15.6 and higher is required!
   proxy_socket_keepalive on;

   proxy_set_header Host $host;
   proxy_set_header X-Real-IP $remote_addr;
   proxy_set_header X-Scheme $scheme;
   proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
   proxy_set_header Accept-Encoding "";
   add_header Front-End-Https on;
   proxy_buffering off;
   proxy_request_buffering off;

   #HSTS
   add_header Strict-Transport-Security 'max-age=63072000; includeSubDomains; preload' always;

   #Disable body size check for file upload/download via WP client/agent, required for large files
   client_max_body_size 0;

 }

 location /admin {
  proxy_pass https://admin;
  proxy_http_version 1.1;

  #IP Filterning, specify required subnets to limit access to the Admin Portal if needed
  #allow 10.0.0.0/8;
  #deny all;

  proxy_set_header Host $host;
  proxy_set_header X-Real-IP $remote_addr;
  proxy_set_header X-Scheme $scheme;
  proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
  proxy_set_header Accept-Encoding "";
  proxy_set_header X-Forwarded-Proto $scheme;
  add_header Front-End-Https on;
  proxy_buffering off;

  #HSTS
  add_header Strict-Transport-Security 'max-age=63072000; includeSubDomains; preload' always;

 }

 location /user {
  proxy_pass https://user;
  proxy_http_version 1.1;
```

```
  #IP Filterning, specify required subnets to limit access to the User Portal if needed
  #allow 10.0.0.0/8;
  #deny all;

  proxy_set_header Host $host;
  proxy_set_header X-Real-IP $remote_addr;
  proxy_set_header X-Scheme $scheme;
  proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
  proxy_set_header Accept-Encoding "";
  add_header Front-End-Https on;
  proxy_buffering off;
  proxy_request_buffering off;


  #HSTS
  add_header Strict-Transport-Security 'max-age=63072000; includeSubDomains; preload' always;

  #Disable body size check for file upload/download via User Portal, required for large files
  client_max_body_size 0;

 }

 location /external {
  proxy_pass https://external;
  proxy_http_version 1.1;

  proxy_set_header Host $host;
  proxy_set_header X-Real-IP $remote_addr;
  proxy_set_header X-Scheme $scheme;
  proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
  proxy_set_header Accept-Encoding "";
  add_header Front-End-Https on;
  proxy_buffering off;


  #HSTS
  add_header Strict-Transport-Security 'max-age=63072000; includeSubDomains; preload' always;

  #Disable body size check for file download via the External Portal, required for large files
  client_max_body_size 0;

 }
}
```